

Westcoast Customer Interface Multi-Factor Authentication (MFA) Enrollment Guide

July 2024

Contents

Westcoast Customer Interface Multi-Factor Authentication Enrollment.....	2
Accessing Westcoast Customer Interface	2
MFA Setup Process	3
1. Okta Verify Setup	4
2. Google Authenticator Setup	5
3. SMS Authentication	6
4. Voice Call Authentication.....	6
Setting Up Multiple Authentication Factors	7
Need your MFA Reset?.....	8
Need more help?	8

Westcoast Customer Interface Multi-Factor Authentication Enrollment

As part of ongoing efforts to ensure safe and reliable operations, Enbridge has included Multi-Factor Authentication (MFA) to the Westcoast Customer Interface (CI) website. Users will be required to provide two forms of evidence of validation during the login process.

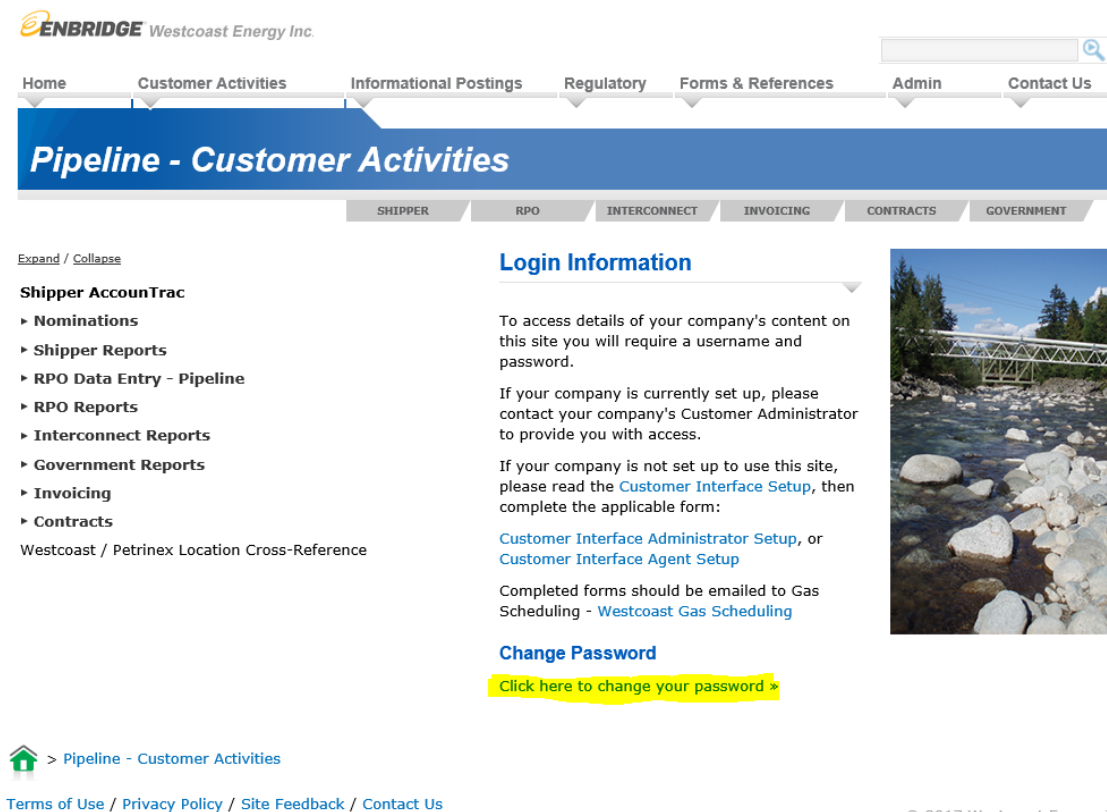
Enbridge uses Okta as the service provider for Multi-Factor Authentication. This document explains how to set up MFA to access the CI website.

If you experience issues, please contact the Scheduling Hotline at 1-403-699-1600.

Accessing Westcoast Customer Interface

Access to secured areas of the Customer Interface require a User ID and password. If it is your first time accessing the CI, please contact your Company Administrator to set up your User ID.

Once your Company Administrator provides you with a CI User ID and Password, you will need to log into CI using the Password provided to you by the Administrator and change your Password before proceeding with MFA Setup Process.



The screenshot shows the Westcoast Customer Interface website. At the top is the Enbridge logo and the text "Westcoast Energy Inc.". Below this is a navigation bar with links: Home, Customer Activities, Informational Postings, Regulatory, Forms & References, Admin, and Contact Us. A large blue banner reads "Pipeline - Customer Activities". Below the banner is a sub-navigation bar with links: SHIPPER, RPO, INTERCONNECT, INVOICING, CONTRACTS, and GOVERNMENT. On the left side, there is a sidebar with a list of links under the heading "Shipper AccountTrac": Nominations, Shipper Reports, RPO Data Entry - Pipeline, RPO Reports, Interconnect Reports, Government Reports, Invoicing, and Contracts. Below this list is a link to "Westcoast / Petrinex Location Cross-Reference". On the right side, there is a section titled "Login Information" with a dropdown arrow. Below this section, there is text explaining that users need a username and password, and if they are not set up, they should contact their Company Administrator. There are links for "Customer Interface Administrator Setup" and "Customer Interface Agent Setup". Below this, there is text stating that completed forms should be emailed to Gas Scheduling - Westcoast Gas Scheduling. There is a link for "Change Password" and a highlighted button that says "Click here to change your password »". On the far right, there is a photograph of a bridge over a river.

ENBRIDGE Westcoast Energy Inc.

Home Customer Activities Informational Postings Regulatory Forms & References Admin Contact Us

Pipeline - Customer Activities

SHIPPER RPO INTERCONNECT INVOICING CONTRACTS GOVERNMENT

Expand / Collapse

Shipper AccountTrac

- Nominations
- Shipper Reports
- RPO Data Entry - Pipeline
- RPO Reports
- Interconnect Reports
- Government Reports
- Invoicing
- Contracts

Westcoast / Petrinex Location Cross-Reference

Login Information

To access details of your company's content on this site you will require a username and password.

If your company is currently set up, please contact your company's Customer Administrator to provide you with access.


If your company is not set up to use this site, please read the [Customer Interface Setup](#), then complete the applicable form:


[Customer Interface Administrator Setup](#), or [Customer Interface Agent Setup](#)

Completed forms should be emailed to Gas Scheduling - [Westcoast Gas Scheduling](#)

Change Password

[Click here to change your password »](#)



 > Pipeline - Customer Activities

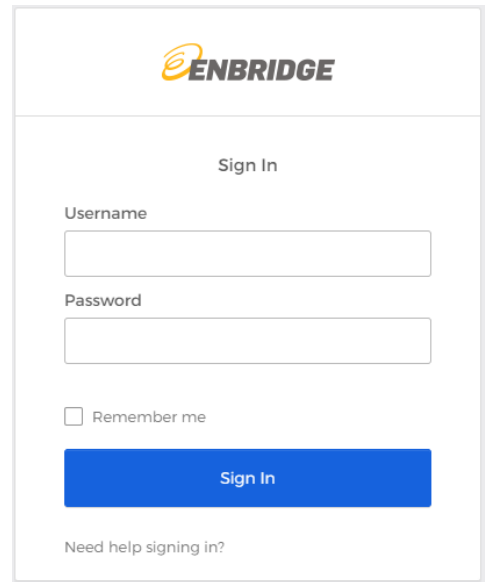
[Terms of Use](#) / [Privacy Policy](#) / [Site Feedback](#) / [Contact Us](#)

© 2017 Westcoast Energy Inc.

MFA Setup Process

1. Sign In:

When accessing secure areas of CI, Users will be prompted to Sign In with their Username and Password.



The Sign In form features the ENBRIDGE logo at the top. Below it, the text "Sign In" is centered. There are two input fields: "Username" and "Password". Below the Password field is a checkbox labeled "Remember me". A blue "Sign In" button is positioned below the checkbox. At the bottom, there is a link that says "Need help signing in?".

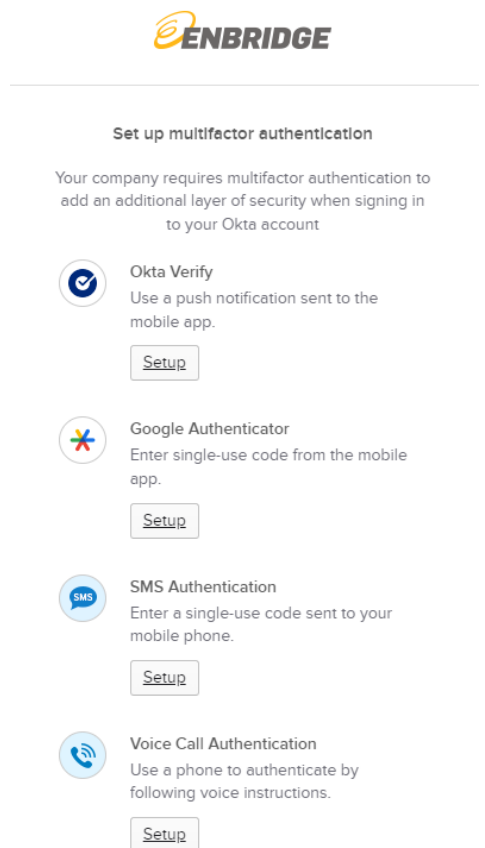
2. Select Factor:

Select one of the four enrollment options available. Proceed to the following pages based on the factor selected.

Okta Verify	Page 4
Google Authenticator	Page 5
SMS Authenticator	Page 6
Voice Call Authenticator	Page 6
Setup Multiple Factors	Page 7

Call the Scheduling Hotline at 1-403-699-1600 if you require more than one factor, wish to reset your factors, or have any issues with the setup process.

Click "Setup" once you have determined which method for authentication you would like to use. Proceed to the appropriate section for instructions.



The "Set up multifactor authentication" screen displays the ENBRIDGE logo at the top. Below the logo, the heading "Set up multifactor authentication" is followed by a message: "Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account". There are four options, each with an icon, a title, a description, and a "Setup" button:

- Okta Verify**: Use a push notification sent to the mobile app.
- Google Authenticator**: Enter single-use code from the mobile app.
- SMS Authentication**: Enter a single-use code sent to your mobile phone.
- Voice Call Authentication**: Use a phone to authenticate by following voice instructions.

1. Okta Verify Setup

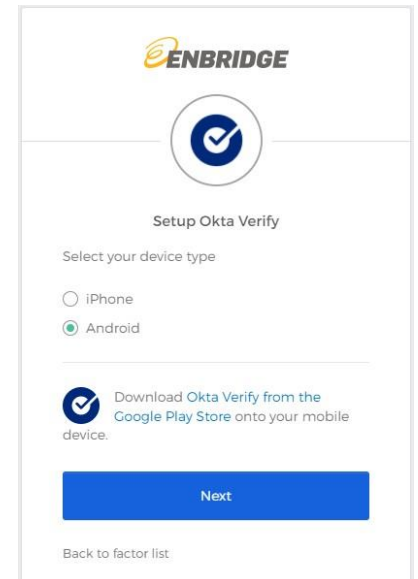
1. Select your device type.

From your phone:

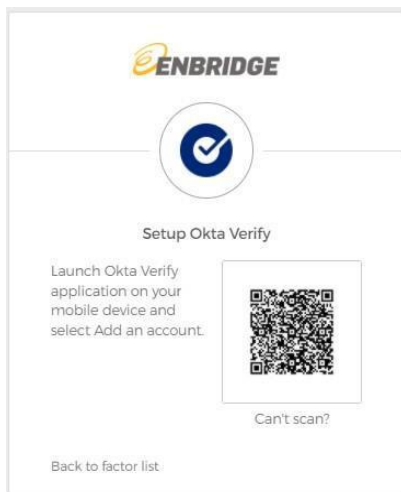
- Download the Okta Verify app from the App Store or the Google Play Store.
- Open the app and tap the “+” to add an account.
- Choose an account type of “Organization”.
- Click “Yes, ready to scan” in the app

On your computer:

- Click Next in the Setup Okta Verify screen to bring up the QR code.

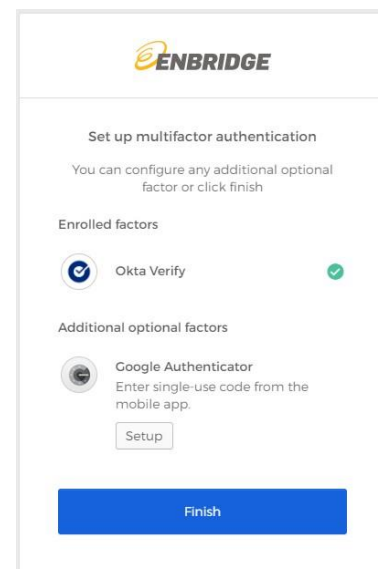


2. Setup Okta Verify by scanning the QR code on your computer using the Okta Verify app on your smartphone.



3. Okta Verify will now show as an enrolled factor.

At this point in the process, you can choose to set up additional factors.



2. Google Authenticator Setup

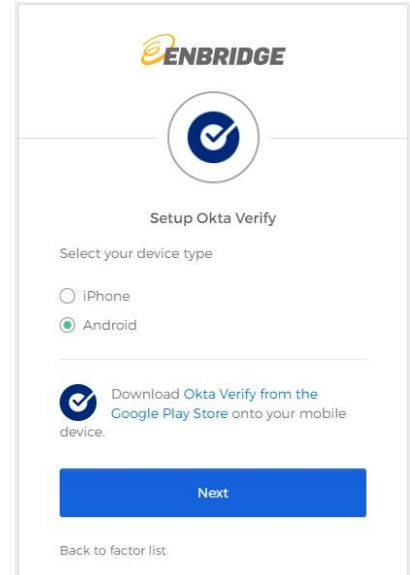
1. Select your device type.

From your phone:

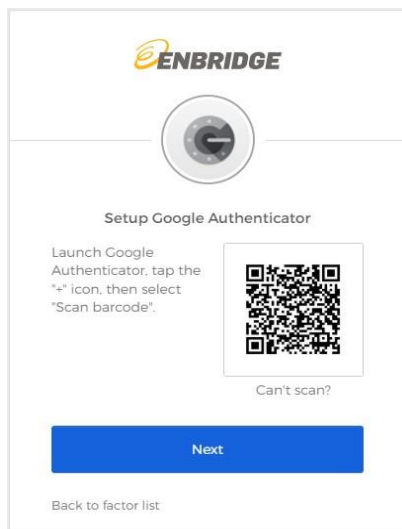
- Install the Google Authenticator app from the App Store or the Google Play Store.
- Open the app on your phone and tap the “+” to add an account.
- Select “Scan QR Code”

On your computer:

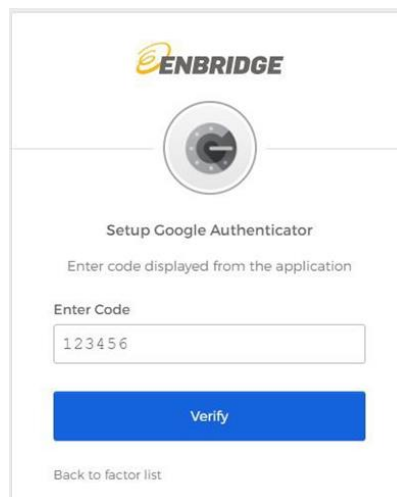
- Click Next and a QR code will be displayed.



2. Setup Google Authenticator by scanning the QR code on your computer using the Google Authenticator app on your smartphone. Once the QR code is scanned successfully, proceed to click “Next” in the panel shown above.

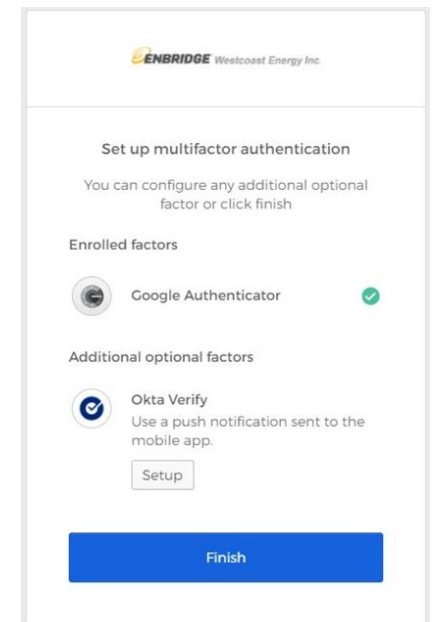


3. Enter the 6-digit code from the Google Authenticator app and click “Verify”:



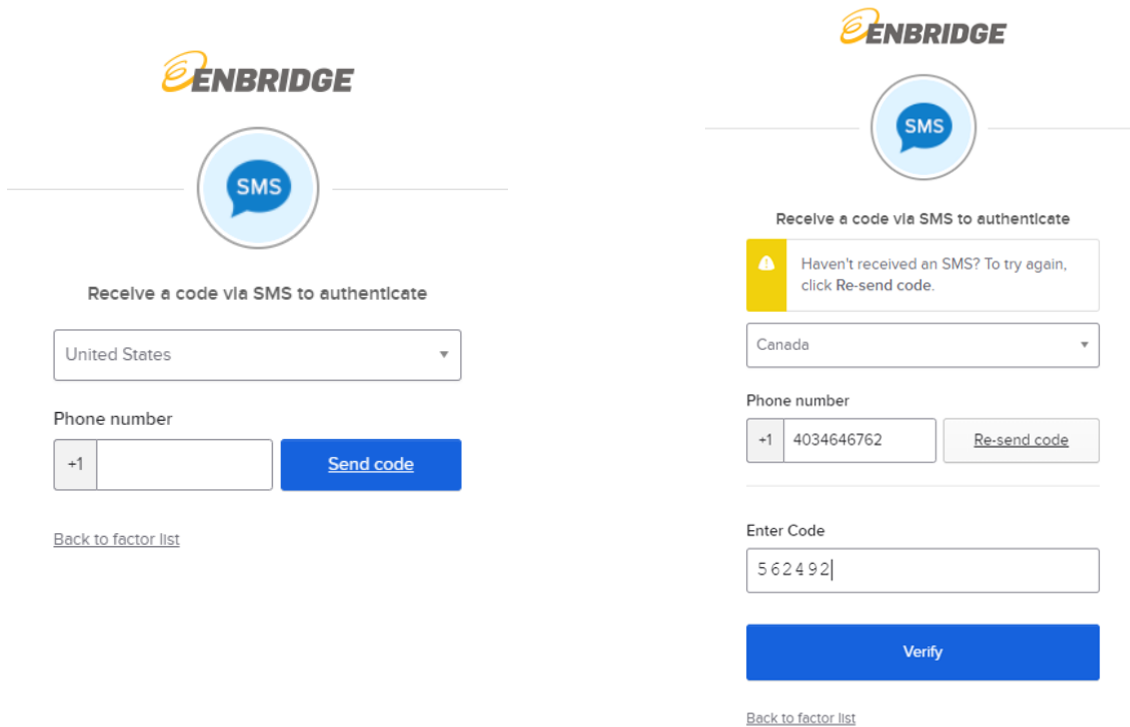
4. Google Authenticator will now show as an enrolled factor.

At this point in the process, you can choose to set up additional factors.



3. SMS Authentication

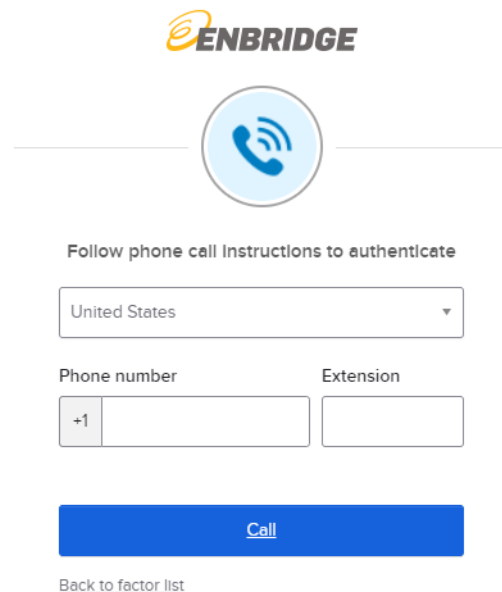
To setup SMS Authentication, you will need to select your Country and enter your phone number, then click “Send code”. You will receive a text message with a code which you will need to enter for verification.



The image displays two screenshots of the ENBRIDGE SMS authentication interface. The left screenshot shows the initial setup screen with the ENBRIDGE logo, an SMS icon, and the heading "Receive a code via SMS to authenticate". It includes a dropdown menu for "United States", a "Phone number" field with a "+1" prefix and a "Send code" button, and a "Back to factor list" link. The right screenshot shows the verification screen with the ENBRIDGE logo, an SMS icon, and the heading "Receive a code via SMS to authenticate". It includes a yellow warning box with the text "Haven't received an SMS? To try again, click Re-send code.", a dropdown menu for "Canada", a "Phone number" field with a "+1" prefix and a "Re-send code" button, an "Enter Code" field with the code "5 6 2 4 9 2", a "Verify" button, and a "Back to factor list" link.

4. Voice Call Authentication

To setup Voice Call Authentication, you will need to select your Country and enter your phone number. Click “Call” and enter the code that you heard over the phone.

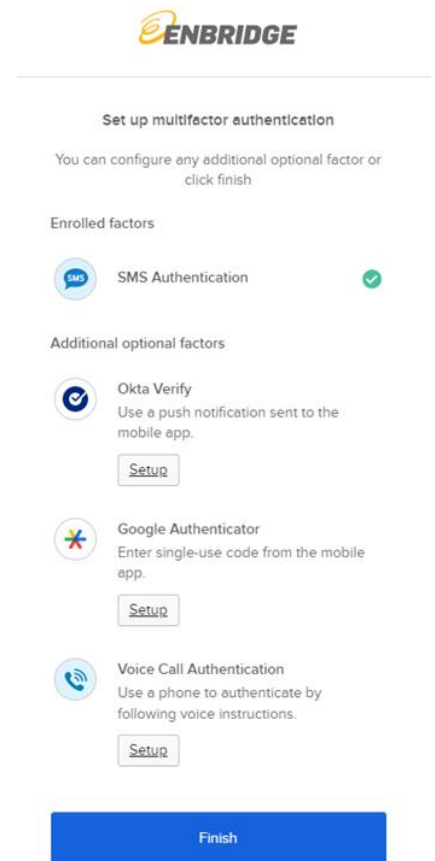



The image displays the ENBRIDGE Voice Call authentication setup screen. It features the ENBRIDGE logo, a voice call icon, and the heading "Follow phone call instructions to authenticate". Below this is a dropdown menu for "United States", a "Phone number" field with a "+1" prefix, an "Extension" field, and a "Call" button. A "Back to factor list" link is located at the bottom.

Setting Up Multiple Authentication Factors

Upon setting up a Multifactor Authentication Factor you will have the option to setup additional Factors.

Once you have completed setting up the Factors you would like to use click on “Finish.”










Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

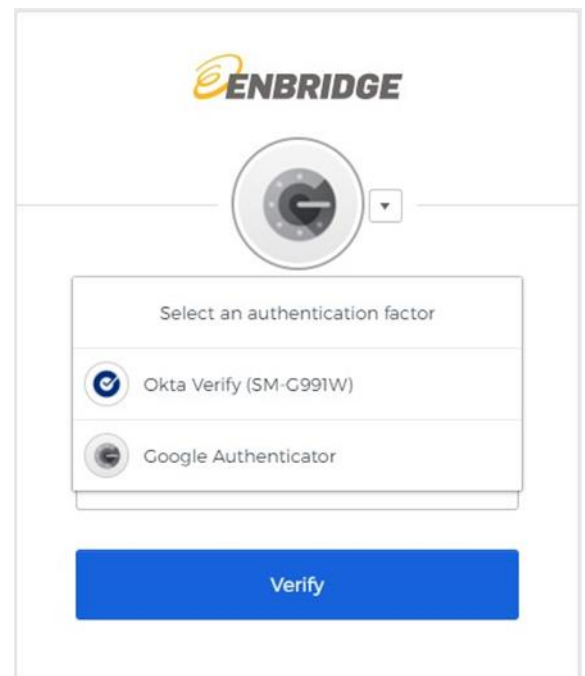
-  SMS Authentication 


Additional optional factors


-  Okta Verify
Use a push notification sent to the mobile app.
[Setup](#)
-  Google Authenticator
Enter single-use code from the mobile app.
[Setup](#)
-  Voice Call Authentication
Use a phone to authenticate by following voice instructions.
[Setup](#)

[Finish](#)



If you have set up more than one factor, select the dropdown arrow beside the authenticator icon in this panel to switch between factors.







Select an authentication factor

-  Okta Verify (SM-G991W)
-  Google Authenticator

[Verify](#)

Need your MFA Reset?

You may require an MFA Reset in the event you get a new device or don't have your cell phone in your possession and need to select an alternate MFA Factor. Contact your Company Administrator to reset your MFA. Once your MFA is reset, please click on a link that is secure (a link that you need to use your User ID and Password) and you will be prompted to set up the MFA once again. An example is clicking on the Nomination Maintenance link. NOTE: You **Do Not** need to reset your password to reset your MFA.

CSR Hotline 1-403-699-1800
Scheduling Hotline 1-403-699-1600

ENBRIDGE Westcoast Energy Inc.

Home Customer Activities Informational Postings Regulatory Forms & References Admin Contact Us

Pipeline - Customer Activities

SHIPPER RPO INTERCONNECT INVOICING CONTRACTS GOVERNMENT

[Expand / Collapse](#)

Shipper AccountTrac

- ▼ **Nominations**
 - Nominations Maintenance**
 - Transporter Nominations Import
 - Late Day Nominations Maintenance
 - EPSQ Forecaster
- Shipper Reports
- RPO Data Entry - Pipeline
- RPO Reports
- Interconnect Reports
- Government Reports
- Invoicing
- Contracts

Westcoast / Petrinex Location Cross-Reference

Login Information

To access details of your company's content on this site you will require a username and password.

If your company is currently set up, please contact your company's Customer Administrator to provide you with access.


If your company is not set up to use this site, please read the [Customer Interface Setup](#), then complete the applicable form:

[Customer Interface Administrator Setup](#), or
[Customer Interface Agent Setup](#)

Completed forms should be emailed to Gas Scheduling - [Westcoast Gas Scheduling](#)

Change Password

[Click here to change your password »](#)



Need more help?

If you have further questions, please call the Scheduling Hotline at 1-403-699-1600 or toll free at 1-877-675-6747.